FACTORIAL RINGS AND DIAGONAL REDUCTION OF MATRICES

R. Miralles* , P. Rubió † and E. Ventura‡

March 1997

Abstract

The class of Bézout factorial rings is introduced and characterized. Using the factorial properties of such a ring R, and given a $n \times m$ matrix A over R, we find $P \in GL(n, R)$ and $Q \in GL(m, R)$ such that PAQ is diagonal with every element in the diagonal dividing the following one.

Key-words: Ring, Bézout, principal, factorization, reduction of matrices.

1 Introduction

The irreducibility of elements in a ring is a classical concept in commutative ring theory. A non-unit element x in a ring R is called irreducible when $x = ab$ forces a or b to be a unit. And a ring R is called factorial when every non-zero non-unit element in R can be decomposed as a product of irreducible elements. Classical examples of factorial rings are the principal ideal domains (for example the ring of integers) in which, furthermore, the factorization of an element is essentially unique (that is, a principal ideal domain is a unique factorization domain, see [2]).

A ring R is an *elementary divisor* ring when for every (non necessarily square) matrix A over R, there exist two invertible matrices of suitable sizes P and Q such that PAQ is a diagonal matrix with every element in the diagonal dividing the following one (see [3] particularized to the conmutative case). As it is mentioned in [3], the definition of elementary divisor ring can be used to easily derive an structure theorem for finitely presented modules over such a ring. And the first example of elementary divisor rings are the principal ideal domains (see [2]); the case of the integers gives us the wellknown classification of finitely generated abelian groups. In [3] (see Theorem 12.3), Kaplansky give a powerfull structure

[1]Esc. Univ. Pol. Man. (UPC).
[2]Esc. Univ. Pol. Man. (UPC). e-mail: rubio@bages.eupm.upc.es
[3]Esc. Univ. Pol. Man. (UPC). e-mail: ventura@ma3.upc.es

theorem for (commutative) principal ideal rings. And as an easy corollary, it follows that every principal ideal ring is an elementary divisor ring.

In this paper we generalize the concept of irreducible element. With respect to this extended concept we give the corresponding notion of factorial ring, which includes rings that are not factorial in the classical sense. The theory developed here is in between the classical divisibility theory for principal ideal domains, and the also classical theory on primary decomposition of ideals in noetherian rings (see [1]). In section 1, we play attention to the Bézout factorial rings, in which we analize the behavior of the possibly different factorizations of a given element. In section 2 we prove that every Bézout factorial ring is a principal ideal ring; and we give a structure theorem for Bézout factorial rings (Theorem 8). Finally, in section 3, we use the properties of the factorizations to prove that every Bézout factorial ring is an elementary divisor ring. Althought this is not a new result (it is contained in the corollary of Theorem 12.3 in [3] mentioned above), the proof provided here does not use the structure theorem and works directly with elements and their factorizations.

In all this paper, every ring is assumed to be conmutative and with unit.

2 Definitions and first properties

Definition 1 Extending the definition in [3], we say that two elements x, $y \in R$ are *associates*, denoted $x \equiv y$, when they are multiples of each other, that is, when they generate the same principal ideal, $xR = yR$. For example, $x \equiv 1$ if and only if x is a unit in R.

The divisibility relation will be denoted by $|$; that is, $y \,|\, x$ if and only if $x = yz$ for some $z \in R$. The greatest common divisor of two elements x and y (that is, the generator of the ideal $xR + yR$), in case it exist, will be denoted $\gcd(x, y)$. Of course, it is only defined up to associates.

An element $p \in R$ is said to be *irreducible* when p is not a unit and for every $x \,|\, p$, either x is a unit or $x \equiv p$. Equivalently, p is irreducible if and only if pR is maximal as a proper principal ideal in R.

As a *decomposition* of an element $x \in R$ we mean an expression of the type $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $r \geq 0$ and, for every $i = 1, \cdots, r$, p_i is an irreducible element and $\alpha_i \geq 0$ (it will be understood that the empty expression, i.e. that corresponding to $r = 0$, is a decomposition of the units in R, that is $1 \equiv\ $). The length of such an expression is $\sum_{i=1}^{r} \alpha_i$, denoted l (and we assume that the length of the empty expression is zero). We say that a decomposition of x, $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, is *normalized* when $p_i \equiv p_j$ if and only if $i = j$, and $\alpha_i > 0$ for $i = 1, \cdots, r$. Of course, by deleting the terms with zero exponent and collecting together the possibly different associate terms, if an element $x \in R$ has a decomposition then it has a normalized decomposition too.

Two normalized decompositions of a given element, $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $x \equiv q_1^{\beta_1} \cdots q_s^{\beta_s}$,

are considered to be equal when $r = s$ and, up to reordering the indices, $p_i \equiv q_i$ and $\alpha_i = \beta_i$ for every $i = 1, \cdots, r$. In other words, when we consider the decomposition $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, we are writting elements but we are thinking in the corresponding decomposition of xR as a product of maximal proper principal ideals $xR = (p_1 R)^{\alpha_1} \cdots (p_r R)^{\alpha_r}$.

Consider two decompositions of elements in R, $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $y \equiv q_1^{\beta_1} \cdots q_s^{\beta_s}$, say γ_x and γ_y respectively. We say that γ_x is *shorter* than γ_y, denoted $\gamma_x \leq \gamma_y$, when $r \leq s$ and, up to reordering the indices, $p_i \equiv q_i$ and $\alpha_i \leq \beta_i$ for every $i = 1, \cdots, r$. Clearly, if $\gamma_x \leq \gamma_y$ then $x \,|\, y$. And, in case they are normalized, $\gamma_x \leq \gamma_y$ and $\gamma_y \leq \gamma_x$ if and only if γ_x and γ_y are the same decomposition (and in this case, $x \equiv y$).

The ring R is called *factorial* when every $0 \neq x \in R$ has a decomposition (and so, a normalized decomposition).

Remark 2 With some conditions on R (for example, if R is a domain), $x \equiv y$ implies $x = uy$ for some unit $u \in R$. But in general, this is not true (see 2 in [3] for counterexamples).

If $p \in R$ is such that $p = ab$ forces a or b to be a unit (that is, if p is "irreducible" in the classical sense) then p is irreducible. But the convers is not true. Take, for example, an arbitrary ring R and a field K, and consider $(0, 1) \in K \times R$. Clearly $(0, 1)K \times R$ is maximal as a proper principal ideal in $K \times R$ but $(0, 1)$ is idempotent and it is not a unit in $K \times R$.

Every factorial ring in the classical sense is factorial in the sense of Definition 1. But the convers is again not true. Take, for example, two fields K_1 and K_2 and consider $R = K_1 \times K_2$. The unique irreducible elements of R in the classical sense are the units (and so R is not factorial in the classical sense). Otherwise, in our sense, $(1, 0)$ and $(0, 1)$ are irreducible elements and every non-zero element in R is either a unit or it is associate to $(1, 0)$ or to $(0, 1)$. So, R is factorial in the sense of Definition 1.

Example 3 Consider the ring of integers modulo $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $R = \mathbb{Z}/n\mathbb{Z}$, which is a principal ideal ring. Let us denote the class of $a \in \mathbb{Z}$ by $\overline{a}$. The maximal ideals in R are precisely $\overline{p_i}R$, $i = 1, \cdots, r$. So, the irreducible elements in R are $\overline{p_i}$, $i = 1, \cdots, r$. Given now an arbitrary element, $\overline{m} \in R$, we can decompose it in the following way. Consider $d = \gcd(m, n)$ and write $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ and $m = m'd$, for some exponents $0 \leq \beta_i \leq \alpha_i$, $i = 1, \cdots, r$ and some $m' \in \mathbb{Z}$ with $\gcd(m', n) = 1$. We have $\overline{m} = \overline{m'}\overline{p_1}^{\beta_1} \cdots \overline{p_r}^{\beta_r} \equiv \overline{p_1}^{\beta_1} \cdots \overline{p_r}^{\beta_r}$ because $\overline{m'}$ is a unit in R. Thus, R is a factorial ring.

Lemma 4 *Let R be a Bézout factorial ring.*

(i) If $x \,|\, yz$ and $gcd(x, y) = 1$ then $x \,|\, z$.

(ii) if $p, q \in R$ are irreducible elements then either $p \equiv q$ or $gcd(p, q) = 1$ (and not both).

(iii) If p and q are two irreducible elements in R and $p \,|\, q^r$ for some $r \geq 1$ then $p \equiv q$.

(iv) *If $p \in R$ is irreducible and nilpotent then p is the unique irreducible element in R up to associates; furthermore, for every $x \in R$, either $x = 0$ or x is a unit or $p \,|\, x$.*

(v) *If p and q are irreducible elements of R with $p \not\equiv q$ then $gcd(p^r, q^s) = 1$ for every $r, s \geq 0$.*

Proof. Suppose that $x \,|\, yz$ and $\gcd(x, y) = 1$ and write $yz = ax$ and $1 = bx+cy$ for some $a, b, c \in R$. Multiplying the second equation by z we obtain $z = bxz + cyz = bxz + cax = x(bz + ca)$. This proves *(i)*.

Let p and q be two irreducible elements in R and consider $d = \gcd(p, q)$. $d \,|\, p$ and $d \,|\, q$ so, either d is a unit or $p \equiv d \equiv q$. This proves *(ii)*. Using *(i)* and *(ii)* and an inductive argument on r we deduce *(iii)*. And applying *(iii)* we obtain the uniqueness in *(iv)*. The fact that R is a factorial ring completes now the proof of *(iv)*.

Suppose now that p and q are irreducible elements of R with $p \not\equiv q$, take $r, s \geq 1$ and consider $d = \gcd(p^r, q^s)$. By *(iv)*, $p^r \neq 0$ and $q^s \neq 0$ and so $d \neq 0$. If d is not a unit then d must be multiple of some irreducible element h. Now, $h \,|\, p^r$, $h \,|\, q^s$ and by *(iii)* we obtain the contradiction $p \equiv h \equiv q$. Thus, $d = 1$ and *(v)* is proven.

Proposition 5 *Let R be a Bézout factorial ring.*

(i) *There exist a unique normalized decomposition of every $0 \neq x \in R$ with minimal length. It will be called the distinguished decomposition of x, denoted γ_x; and we will refer to $l(\gamma_x)$ as the length of x, $l(x)$.*

(ii) *For every $0 \neq x \in R$, write $\gamma_x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Every other normalized decomposition γ of x is of the form $\gamma = p_1^{\beta_1} \cdots p_r^{\beta_r}$ for some exponents $\beta_i \geq \alpha_i$, $i = 1, \cdots, r$; in particular, γ_x is shorter than any other normalized decomposition of x.*

(iii) *For every $x, y \in R$, $x, y \neq 0$, we have that $x \,|\, y$ if and only if $\gamma_x \leq \gamma_y$. In this case, $l(x) \leq l(y)$.*

Proof. The existence of normalized decompositions with minimal length is guaranteed by the factorial hypothesis on R. Suppose now that we have two normalized decompositions of some elements $x, y \neq 0$, respectively γ_1 and γ_2. By allowing zero exponents we may assume that they are $x \equiv p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $y \equiv p_1^{\beta_1} \cdots p_r^{\beta_r}$ for some irreducible pairwise non-associate elements $p_1, \cdots, p_r$ and some exponents $\alpha_i, \beta_i \geq 0$ with $\max\{\alpha_i, \beta_i\} \geq 1$, $i = 1, \cdots, r$. Suppose that $x \,|\, y$. Fix i. If $\alpha_i \neq 0$ then $p_i^{\alpha_i} \,|\, x$, so $p_i^{\alpha_i} \,|\, y$ and by induction on r and using Lemma 4*(i)* and 4*(v)* we obtain $p_i^{\alpha_i} \,|\, p_i^{\beta_i}$. In particular, $\beta_i \neq 0$. Simetrizing the argument and recalling that $\alpha_i = \beta_i = 0$ is not the case, we can deduce that if $x \equiv y$ then $\alpha_i \neq 0$, $\beta_i \neq 0$ and $p_i^{\alpha_i} \equiv p_i^{\beta_i}$.

Suppose now that $l(\gamma_1)$ $(= \sum_{i=1}^{r} \alpha_i)$ is the minimal length of normalized decompositions of x. If, for some i, $\alpha_i > \beta_i$ then changing $p_i^{\alpha_i}$ by $p_i^{\beta_i}$ in γ_1, we should decrease $l(\gamma_1)$

contradicting the minimality. So, $\alpha_i \leq \beta_i$ for all $i = 1, \cdots, r$. This simultaniously prove that the normalized decomposition of x with minimal length is unique, say γ_x, and that γ_x is shorter than any other normalized decomposition of x, in which, furthermore, it appear precisely the same irreducible elements that they did in γ_x. So *(i)* and *(ii)* are proven.

It is clear that if $\gamma_x \leq \gamma_y$ then $x \,|\, y$. Conversely, suppose that $x \,|\, y$. The argument in the first paragraph applied to γ_x and γ_y shows that, $\gamma_x \leq \gamma_y$. So, we have *(iii)*.

3 A structure theorem for Bézout factorial rings.

Definition 6 Let R be a commutative ring with unit. A *divisibility valuation* on R is a map $\varphi : R - \{0\} \to \mathbb{N}$ such that whenever $x \,|\, y$, $\varphi(x) \leq \varphi(y)$ and the equality occurs if and only if $x \equiv y$. Observe that if φ is a divisibility valuation on R then φ is constant on the set of units in R and $\varphi(1) = \min_{x \neq 0} \varphi(x)$. Particularizing [3] to the commutative case, we say that R is a *valuation ring* when for every x, $y \in R$ either $x \,|\, y$ or $y \,|\, x$.

It is easy to show that in a valuation ring R, the set of non-units forms the unique maximal ideal, so R is a local ring. It is also easy to show that every ideal in a noetherian valuation ring is principal (in fact, if not take a non-principal ideal I and an element $x \in I$; there must exist $y \in I$ not multiple of x so, $y \,|\, x$, that is $xR \subset yR$. Repeating the argument infinitely many times, we get a contradiction with the noetherian condition). Suppose now that R is an artinian valuation ring. We know that R is principal, local (with maximal ideal, say pR) and furthermore the complete list of ideals in R is $\{0\} = p^n R \subset p^{n-1} R \subset \cdots \subset p^2 R \subset pR \subset R$, for some $n \geq 1$. In fact, we have the mentioned chain in R (see Proposition 8.6 in [1]) and the definition of valuation ring forces every ideal $I = xR$ to be located between two steps of the chain, $p^{r+1}R \subseteq xR \subseteq p^r R$. Now, $x = up^r$ and if $p^{r+1}R \neq xR$ then $u \notin pR$ so u is a unit and then $xR = p^r R$.

Proposition 7 *(i) Every Bézout factorial ring has a divisibility valuation.*

(ii) Every Bézout ring with a divisibility valuation is a principal ideal ring.

Proof. Using Proposition 5, it is easy to show that in a Bézout factorial ring the length of elements is a divisibility valuation. This proves *(i)*. Let now R be a Bézout ring with a divisibility valuation φ and let $I \neq 0$ be an ideal of R. Let $0 \neq x \in I$ be an element in I with $\varphi(x)$ minimal. For every other $0 \neq y \in I$ we can consider $d = \gcd(x, y)$. We have that $d \,|\, x$ and so $\varphi(d) \leq \varphi(x)$. But $d \in I$. Then, by minimality, $\varphi(d) = \varphi(x)$ and so $d \equiv x$. Thus, $x \,|\, y$. This prove that $I = xR$ and that I is principal.

Theorem 8 *Let R be a commutative ring with unit. The following are equivalent:*

(a) R is a Bézout factorial ring,

(b) R is a Bézout ring with a divisibility valuation,

(c) either R is a principal ideal domain or R is isomorphic to a finite product of fields and artinian valuation rings,

(d) R is a principal ideal ring in which every prime ideal is maximal.

(e) R is a principal ideal ring which is a domain or it has a finite number of ideals.

Proof. By Proposition 7*(i)*, *(a)* implies *(b)*. Suppose that R is a Bézout ring with a divisibility valuation, say φ. By Proposition 7*(ii)*, R is a principal ideal ring and by Theorem 12.3 of [3], R is (isomorphic to) a finite product of (principal ideal) domains and artinian valuation rings, say

$$R \simeq D_1 \times \cdots \times D_r \times K_1 \times \cdots \times K_s \times V_1 \times \cdots \times V_t$$

where r, s, $t \geq 0$, the D_i's are domains and not fields, the K_i's are fields and the V_i's are artinian valuation rings. Suppose that $r+s+t \geq 2$ and that $r \geq 1$, and consider the element $x = (0, 1, \cdots, 1) \in R$. Take p a prime element in D_1 and consider $y = (p, 1, \cdots, 1) \in R$. It is clear that different powers of y are not associate in R. But $x = xy^n$ and so $\varphi(y^n) \leq \varphi(x)$ for every n. Then, $\varphi(x)$ is a natural number bigger than infinitely many natural numbers, a contradiction. Thus, either $r + s + t = 1$ or $r = 0$. This proves that *(b)* implies *(c)*.

It is clear that the trivial ring $R = 1$ and every principal ideal domain are Bézout factorial rings. Suppose that $R = K_1 \times \cdots \times K_s \times V_1 \times \cdots \times V_t$ for some s, $t \geq 0$, $s+t \geq 1$, some fields K_i and some artinian valuation rings V_i. Denote by p_i the generator of the maximal ideal in V_i (that is the unique irreducible element in V_i up to associates); and denote by n_i the nilpotency index of p_i. It is easy to prove that an element $(x_1, \cdots, x_{r+s}) \in R$ is irreducible if and only if there is an index j such that, x_i is a unit for every $i \neq j$ and $x_j = 0$ if $1 \leq j \leq r$, or $x_j \equiv p_j$ if $r + 1 \leq j \leq r + s$. Consider now an arbitrary non-zero element $x = (x_1, \cdots, x_{r+s}) \in R$. For every $i = 1, \cdots, r$ either $x_i = 0$ or x_i is a unit; and for every $i = r + 1, \cdots, r + s$ we have $x_i = u_i p_i^{\alpha_i}$ for some unit u_i and some $0 \leq \alpha_i \leq n_i$. So, every $x \in R$ can be decomposed as a product of irreducible elements in R. This proves that R is a factorial ring. And clearly R is a Bézout ring. So *(c)* implies *(a)*.

Suppose now that R is like in *(c)*. Every ideal I in R is of the form $I = I_1 \times \cdots \times I_{r+s}$ when if $1 \leq i \leq r$ we have $I_i = 0$ or $I_i = K_i$, and if $r+1 \leq i \leq r+s$ then $I_i = p_i^{\alpha_i} V_i$ for some $0 \leq \alpha_i \leq n_i$. So, it is clear that I is prime if and only if it is maximal. That is, *(c)* implies *(d)*. Suppose now that R is a principal ideal ring for which every prime ideal is maximal. We have the above description of R given by Theorem 12.3 of [3] and we further know that if a quotient of R is a domain then it is a field. This implies that either $r + s + t = 1$ or $r = 0$. So, *(d)* implies *(c)*.

Finally, every field and every artinian valuation ring have a finite number of ideals while a principal ideal domain which is not a field has infinitely many. So, *(c)* $\Leftrightarrow$ *(e)*.

Corollary 9 *Every finite principal ideal ring is factorial.*

Corollary 10 *Every principal ideal ring can be embedded in a Bézout factorial ring that is in a principal ideal ring in which every prime ideal is maximal.*

Proof. Let R be a principal ideal ring and consider the description of R given by Theorem 12.3 of [3] (use the notation above). Then, R can be embedded into $R' = Q_1 \times \cdots \times Q_r \times K_1 \times \cdots \times K_s \times V_1 \times \cdots \times V_t$ where Q_i is the field of fractions of D_i, $i = 1, \cdots, r$. By Theorem 8, R' is a Bézout factorial ring or, in other words, a principal ideal ring for which every prime ideal is maximal.

It is not obvious from the definitions that every element in a Bézout factorial ring should have a decomposition (in fact, we know it does but only up to associates). We can now prove this as a corollary of Theorem 8.

Corollary 11 *Let R be a Bézout factorial ring. Then, $x \equiv y$ if and only if $x = uy$ for some unit $u \in R$. Consequently, every element $0 \neq x \in R$ has a decomposition $x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Furthermore, for every pair of non-zero elements $x, y \in R$, write $d = gcd(x, y)$, and then there exist $x', y', \lambda, \mu \in R$ with $gcd(x', y') = 1$ and $gcd(\lambda, \mu) = 1$, such that $x = dx'$, $y = dy'$ and $d = \lambda x + \mu y$.*

Proof. The first assertion is clear in light of Theorem 8 *(a)* $\Leftrightarrow$ *(c)* (in fact, it is true in every principal ideal ring). And the second assertion is now clear.

Let γ_1 and γ_2 be decompositions of some non-zero elements $x, y \in R$. We have decompositions $x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $y = p_1^{\beta_1} \cdots p_r^{\beta_r}$ for some irreducible pairwise non-associate elements $p_1, \cdots, p_r \in R$ and some exponents $\alpha_i, \beta_i \geq 0$ with $\max\{\alpha_i, \beta_i\} \geq 1$, $i = 1, \cdots, r$. By Proposition 5*(iii)*, $p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}}$ is a greatest common divisor of x and y, so we may assume $d = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}}$. Now, take $x' = p_1^{\alpha_1 - \min\{\alpha_1, \beta_1\}} \cdots p_r^{\alpha_r - \min\{\alpha_r, \beta_r\}}$ and $y' = p_1^{\beta_1 - \min\{\alpha_1, \beta_1\}} \cdots p_r^{\beta_r - \min\{\alpha_r, \beta_r\}}$. We have $x = dx'$, $y = dy'$ and, by Lemma 4, $\gcd(x', y') = 1$. Finally, consider the following Bézout identity (with the previous result applied to the two coefficients), $d = \alpha\lambda x + \alpha\mu y$ for some $\alpha, \lambda, \mu \in R$ with $\gcd(\lambda, \mu) = 1$. We have $d = d\alpha(\lambda x' + \mu y')$. Thus, $d \equiv d(\lambda x' + \mu y')$ that is $d = ud(\lambda x' + \mu y') = (u\lambda)x + (u\mu)y$ for some unit $u \in R$. This completes the proof.

4 Diagonal reduction of matrices

Let us now use the factorizations of elements (or, for notational convenience, the divisibility valuation) in a Bézout factorial ring R to compute the diagonal reduction of a given $n \times m$ matrix A over R. We say that A *admits diagonal reduction* if and only if there exist $P \in GL(n, R)$ and $Q \in GL(m, R)$ such that PAQ is a diagonal matrix (i.e. has zeros in all the entries outside the main diagonal) and with every element in the diagonal dividing the

following one. By Theorem 9.3 in [3] (which is valid in general for an arbitrary commutative ring), this diagonal reduction, in case it exists, is essentially unique. That is, if $PAQ = \mathrm{diag}(a_1, \cdots, a_r)$ and $P'AQ' = \mathrm{diag}(b_1, \cdots, b_r)$ with the above properties then $a_i \equiv b_i$ for every $i = 1, \cdots, r = \min\{n, m\}$. The elements in the diagonal reduction, defined up to associates, are called the *invariant factors* of A. A ring R is called an *elementary divisor* ring when every matrix over R has diagonal reduction.

In [3], the author says that, as an immediate corollary of the structure theorem for principal ideal rings (Theorem 12.3), it can be deduced that every principal ideal ring is an elementary divisor ring. However, this proof is very indirect since it passes through the mentioned structure theorem. We give here an alternative proof of the fact that every Bézout factorial ring is an elementary divisor ring which works directly with matrices, playing with the factorizations of those elements in.

Theorem 5.1 in [3], asserts that if every 1×2, 2×1 and 2×2 matrices over a ring R admit diagonal reduction then every matrix over R also does, and so R is an elementary divisor ring. This result is proven with a completely algorithmic inductive argument on the sizes of A. Furthermore, in the commutative case, the diagonal reducibility of 1×2 matrices is equivalent to that of 2×1 matrices, by transposing. So, we can restrict our attention to the cases 1×2 and 2×2.

Theorem 12 *Every Bézout factorial ring is an elementary divisor ring.*

Proof. Let φ be a divisibility valuation on R and, for notational convenience, define $\varphi(0) = +\infty$. Let $A = (a_{i,j})$ be an arbitrary matrix over R and define $\varphi(A) = \min_{i,j} \varphi(a_{i,j})$. We will multiply A in the right and/or in the left by several invertible matrices of suitable size, in such a way that φ never increases. The final result will be a diagonal reduction for A. As we mentioned above, we can restrict to the case 1×2 and 2×2.

Let $A = \begin{pmatrix} a_1 & a_2 \end{pmatrix}$ be a 1×2 matrix over R. Permuting the columns (i.e. right multiplying by the corresponding invertible matrix) if necessary, we may assume that $\varphi(A) = \varphi(a_1)$. Let $d = \gcd(a_1, a_2)$ and, using Corollary 11, write $a_1\alpha + a_2\beta = d$ and $\alpha\alpha' - \beta\beta' = 1$ for some α, β, α', $\beta' \in R$. If $d \not\equiv a_1$ then $\varphi(d) < \varphi(a_1)$ and we have

$$\begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix} \in GL(2, R), \qquad \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix} = \begin{pmatrix} d & a_3 \end{pmatrix}$$

for some $a_3 \in R$ and $\varphi\begin{pmatrix} d & a_3 \end{pmatrix} < \varphi(A)$. Repeating this procedure a finite number of times, we may assume that $d \equiv a_1$, that is, $a_2 = a_1\lambda$ for some $\lambda \in R$. In this case,

$$\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \in GL(2, R), \qquad \begin{pmatrix} a_1 & a_1\lambda \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \end{pmatrix}$$

which satisfies $\varphi\begin{pmatrix} a_1 & 0 \end{pmatrix} = \varphi\begin{pmatrix} a_1 & a_1\lambda \end{pmatrix}$ and gives the diagonal reduction we looked for.

Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ be a 2×2 matrix over R. Permuting the two rows and/or the two columns if necessary, we may assume that $\varphi(A) = \varphi(a_1)$. Consider now $d_i = \gcd(a_1, a_i)$ for $i = 2, 3$. If $d_2 \not\equiv a_1$ then, aplying the previous procedure to the first row, there exist an invertible 2×2 matrix Q such that $\varphi(AQ) < \varphi(A)$. Analogously, if $d_3 \not\equiv a_1$ then there exist an invertible 2×2 matrix P^t such that $\varphi(PA) < \varphi(A)$. So, after a finite number of multiplications, we may assume that $d_2 \equiv a_1 \equiv d_3$, that is we may assume that $a_i = a_1\lambda_i$ for some $\lambda_i \in R$, $i = 2, 3$. In this case,

$$\begin{pmatrix} 1 & 0 \\ -\lambda_3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -\lambda_2 \\ 0 & 1 \end{pmatrix} \in GL(2, R)$$

$$\begin{pmatrix} 1 & 0 \\ -\lambda_3 & 1 \end{pmatrix} \begin{pmatrix} a_1 & a_1\lambda_2 \\ a_1\lambda_3 & a_4 \end{pmatrix} \begin{pmatrix} 1 & -\lambda_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_5 \end{pmatrix}$$

where $a_5 = a_4 - a_1\lambda_2\lambda_3$, and the valuation of the final matrix is at most that of A. Finally, consider $d_5 = \gcd(a_1, a_5)$. If $d_5 \not\equiv a_1$ then adding the second row to the first (i.e. right multiplying by the suitable invertible matrix) and applying the previous procedure we can strictly decrease again the value of φ. So, after a finite number of repetitions of the whole process, we will obtain a diagonal matrix $\mathrm{diag}(a_1, a_5)$ with $d_5 \equiv a_1$ that is with $a_1 \,|\, a_5$. This is the diagonal reduction we looked for.

References

[1] M.F. Atiyah and I.G. Macdonald. *Introducción al Algebra Conmutativa*. Editorial Reverté, 1980.

[2] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Prentice Hall, 1991.

[3] I. Kaplansky. *Elementary Divisors and Modules*. Trans. Amer. Math. Soc, vol.66, pp. 464-491. (1949)